TSA Registered Traveler

Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers

Version 3.0, May 2007

Summary of Changes

Transportation
Security
Administration

RT Registered Traveler™

Summary of Changes

This summary of changes document outlines changes in Version 3.0 of the RT Security, Privacy, and Compliance Standards for Sponsoring Entities and Service Providers.

#	Section/Paragraph	Change	Justification
1	1.2 Definitions Personally Identifiable Information	Updated the Definition of PII, which was previously: "Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person." New definition states: "Any item, collection, or grouping of information about any person that contains: a person's name; a unique identifying number, such as a Social Security, passport, or driver's license number; or other identifying particular assigned to that person, such as a symbol, fingerprint, or photograph."	Updated to clarify what is included as Personally Identifiable Information. The definition was derived from the TSA Management Directive (MD) 2100.2.
2	2.2. System Security Plan	Changed the first sentence of the second paragraph to include third party providers. The sentence now states, "All information systems operated by an SP, **or a third party in support of an SP**, that either directly or indirectly support RT shall be included within the scope of the security privacy and compliance requirements."	Updated to clarify the requirements for subcontractors.
3	Table 3-1	Updated Table 3-1 to reflect the addition of Incident Reporting, Personnel Security, and Privacy Protection.	Necessary to properly reflect the content of section 3.

#	Section/Paragraph	Change	Justification
4	3.1 Privacy Protection	Updated the first paragraph in this section to indicate that SPs shall follow the Fair Information Practice Principles. It now states, “SPs shall establish a written privacy policy to govern the data collected in connection with RT and shall be required to provide this policy, in writing, to each eligible RT Applicant. At a minimum, SPs should follow the Fair Information Practice Principles in developing their privacy policy. Table 3-2 Fair Information Practice Principles provides an overview of the standard. In addition, the SP shall provide each eligible RT Applicant with a copy of the Privacy Act statement supplied by TSA (see Section 3.3.5) at the time of enrollment. SPs shall also review their privacy policy during the annual self assessment. SEs and SPs may adopt privacy policies that are more stringent than required by TSA, however, they may not withhold information requested by TSA.”	The Fair Information Practice Principles were added to the standard to reflect industry best practices.
5	Table 3-2	Created Table 3-2 to describe the Fair Information Practice Principles.	The Fair Information Practice Principles were added to the standard to reflect industry best practices.
6	3.2 Training	Updated the first sentence to include training for all personnel with RT functions, including systems personnel. The sentence now states, “The SE shall develop and conduct a comprehensive training program for all employees who perform **RT functions (e.g., customer service, enrollment and verification personnel, system administrators**, etc.).”	Added to clarify that all personnel with access to the information in the system(s) are required to undergo training.
7	3.3 Personnel Security	Created a new section titled Personnel Security. Includes the following topics: *Initial Submission of SP Key Personnel and Employees* *Addition of Key Personnel and Employees After Launch* *Updates to Key Personnel and Employee Information After Launch* *Removals of Key Personnel and Employees After Launch* *Periodic Reconciliation with TSA* *Communication of Security Vetting Results to SPs*	Added to clearly state RT Personnel Security requirements.

#	Section/Paragraph	Change	Justification
8	3.4.4 Acceptable Documents to Establish Identity and Eligibility	Added the following statement: *"If the RT Applicant submits documents with differing surnames (i.e. married and maiden names), the SP will submit both of the applicant's surnames for TSA review."*	Added to clearly state the requirements for applicants submitting identity documentation with varying surnames.
9	3.5.1 Verification Station Operations	Updated the second paragraph to reflect the CRL procedures identified in the RTIC Specification. It now states, "The SE/SP shall use the most recent RT status results (including the current TSA Security Threat Assessment findings and other eligibility-determining factors) provided by CIMS. A current Card Revocation List (CRL) is maintained within CIMS, and is provided to VPs on a regular basis (every 12 hours) or upon request. VPs are responsible for propagating CRLs received from CIMS to all of their verification stations. It is anticipated that such propagation should only take minutes; however, it is required to occur within 6 hours of receipt from CIMS to accommodate airport operations and offline verification stations. If a verification station has not received an update from CIMS within 24 hours, it must cease to accept RT Participant verification requests, since the station may not have the latest CRL."	Updated to reflect the process defined in the RTIC Specification.
10	3.6 Incident Reporting	Developed Incident Reporting Categories and Reporting Requirements for SPs.	Required to clarify the requirements on SPs in the event of a Security Incident.
11	4. Ongoing Compliance with RT Standards	Added the following bullet point: "The SP's enrollment and verification systems shall be subject to RTIC Technical Interoperability Specification conformance testing by the RT Conformance Lab. Conformance testing is one of the final stages in the process of introducing a new SP into the interoperable RT program. The purpose of conformance testing is to officially certify an SP's technical and procedural ability to comply with all operational and policy requirements outlined in the RTIC Technical Interoperability Specification. SPs must contact TSA to schedule conformance testing and approval from the RT Conformance Lab is required prior to commencing operations."	Required to clarify the need for SP enrollment and verification systems to undergo conformance testing in the RT Conformance Lab.

#	Section/Paragraph	Change	Justification
12	4.3 Review of Compliance Documentation	Changed the last sentence in this section to state “In addition, each SE will require its SP to obtain express written authorization allowing TSA to audit or inspect the security controls over the SP’s RT program, including, performing vulnerability assessments and conformance testing.”	Updated to clarify that TSA is authorized to perform conformance testing on operational RT systems during an audit or inspection.
13	4.4 Baseline Reporting	Added the Baseline Reporting section to outline measurable reporting requirements for enrollment operations, verification station operations and equipment operations.	Required to provide the RT PMO with an understanding of the operational success of the RT Program
14	Appendix A	Updated the acronyms table.	Updated to account for changes in the document.
15	Appendix B	Added “Section 20. Privacy” to address the privacy controls that were created for this version.	Required to address the Fair Information Practice Principles.
16	Appendix C	Changed the title of Appendix C to “Appendix C: Minimum Required RT Security Standards and Procedures for Assessing Compliance with RT Security Standards.”	Updated to better reflect the actual content in the Appendix.
17	Appendix C, page C-1	Added the heading “Minimum Required RT Security Standards,” and created an overview for the controls table.	Added to clarify that the first section of the Appendix focuses on the minimum controls.
18	Appendix C, AC-2 Account Management	Updated the “organization assignment” in the control to now state the following, “The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts **at least annually**.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
19	Appendix C, AC-7 Unsuccessful Login Attempts	Updated the “organization assignment” in the control to now state the following, “The information system enforces a limit of **three** consecutive invalid access attempts by a user during a **30 minute time period**. The information system automatically locks the account/node for **20 minutes** when the maximum number of unsuccessful attempts is exceeded.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.

#	Section/Paragraph	Change	Justification
20	Appendix C, AC-10 Concurrent Session Control	Updated the "organization assignment" in the control to now state the following, "The information system limits the number of concurrent sessions for any user." (Removed "Organization-defined number of sessions")	Required to properly define the minimum controls in accordance with industry best practices.
21	Appendix C, AC-12 Session Termination	Updated the "organization assignment" in the control to now state the following, "The information system automatically terminates a session after **20 minutes** of inactivity."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
22	Appendix C, AT-2 Security Awareness	Updated the "organization assignment" in the control to now state the following, "The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and **annually** thereafter."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
23	Appendix C, AT-3 Security Training	Updated the "organization assignment" in the control to now state the following, "The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and **annually** thereafter."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
24	Appendix C, AU-2 Auditable Events	Updated the "organization assignment" in the control to now state the following, "The information system generates audit records for the following events: **All successful and unsuccessful attempts to access RT networks, network devices, software applications, and systems; activities that might modify, bypass, or negate IT security safeguards; and security-relevant actions associated with processing.**"	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
25	Appendix C, AU-5 Audit Processing	Updated the "organization assignment" in the control to now state the following, "In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: **overwrites the oldest audit records**."	Required to properly define the minimum controls in accordance with industry best practices.

#	Section/Paragraph	Change	Justification
26	Appendix C, AU-11 Audit Retention	Updated the “organization assignment” in the control to now state the following, “The organization retains audit logs **on-line by the system/ network administrator for a minimum of 90 days and archived off-line for a period of 7 years** to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
27	Appendix C, CM-7 Least Functionality	Updated the “organization assignment” in the control to now state the following, “The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of **all unnecessary** functions, ports, protocols, and/or services.”	Required to properly define the minimum controls in accordance with industry best practices.
28	Appendix C, CP-3 Contingency Training	Updated the “organization assignment” in the control to now state the following, “The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training **annually.**”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
29	Appendix C, CP-4 Contingency Plan Testing	Updated the “organization assignment” in the control to now state the following, “The organization tests the contingency plan for the information system **annually using table top exercises** to determine the plan’s effectiveness and the organization’s readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
30	Appendix C, CP-5 Contingency Plan Update	Updated the “organization assignment” in the control to now state the following, “The organization reviews the contingency plan for the information system **annually** and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.

#	Section/Paragraph	Change	Justification
31	Appendix C, CP-9 Information System Backup	Updated the “organization assignment” in the control to now state the following, “The organization conducts backups of user-level and system-level information (including system state information) contained in the information system **daily (incremental) and weekly (full)** and stores backup information at an appropriately secured location.	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
32	Appendix C, IA-4 Identifier Management	Updated the “organization assignment” in the control to now state the following, “The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after **30 days** of inactivity; and (vi) archiving user identifiers.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
33	Appendix C, IR-2 Incident Response Training	Updated the “organization assignment” in the control to now state the following, “The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training **annually.**”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
34	Appendix C, IR-3 Incident Response Testing	Updated the “organization assignment” in the control to now state the following, “The organization tests the incident response capability for the information system **annually** using [Assignment: organization-defined tests and exercises] to determine the incident response effectiveness and documents the results.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
35	Appendix C, MA-6 Timely Maintenance	Updated the “organization assignment” in the control to now state the following, “The organization obtains maintenance support and spare parts for key information system components within **24 hours** of failure.”	Required to properly define the minimum controls in accordance with industry best practices.

#	Section/Paragraph	Change	Justification
36	Appendix C, MP-3 Media Labeling	Updated the “organization assignment” in the control to now state the following, “The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.” Deleted the following: “The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [Assignment: organization-defined list of media types and hardware components].”	Required to properly define the minimum controls in accordance with industry best practices.
37	Appendix C, PE-5 Access Control for Display Medium	Added the following control, “The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.”	Added this control to conform to the requirements of systems at the moderate and high impact levels.
38	Appendix C, PE-8 Access Logs	Updated the “organization assignment” in the control to now state the following, “The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the access logs **monthly**.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
39	Appendix C, PL-3 System Security Plan Update	Updated the “organization assignment” in the control to now state the following, “The organization reviews the security plan for the information system **annually** and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
40	Appendix C, PS-2 Position Categorization	Updated the “organization assignment” in the control to now state the following, “The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations **every 5 years**.”	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.

#	Section/Paragraph	Change	Justification
41	Appendix C, PS-6 Access Agreements	Updated the "organization assignment" in the control to now state the following, "The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements **annually**."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
42	Appendix C, RA-4 Risk Assessment Update	Updated the "organization assignment" in the control to now state the following, "The organization updates the risk assessment **every 3 years**, or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
43	Appendix C, RA-5 Vulnerability Scanning	Updated the "organization assignment" in the control to now state the following, "The organization scans for vulnerabilities in the information system **annually** or when significant new vulnerabilities affecting the system are identified and reported."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.
44	Appendix C, SC-5 Denial of Service Protection	Updated the "organization assignment" in the control to now state the following, "The information system protects against or limits the effects of denial of service attacks." Deleted the following: "[Assignment: organization-defined list of types of denial of service attacks or reference to source for current list]."	Required to properly define the minimum controls in accordance with industry best practices.
45	Appendix C, SC-10 Network Disconnect	Updated the "organization assignment" in the control to now state the following, "The information system terminates a network connection at the end of a session or after **20 minutes** of inactivity."	Required to properly define the minimum controls in accordance with DHS 4300A Sensitive Systems Handbook and TSA MD 1400.3 TSA Information Security Policy.

#	Section/Paragraph	Change	Justification
46	Appendix C, Page C-19	Added the following Privacy controls: • PR-1 Openness • PR-2 Collection Limitation • PR-3 Purpose Specification • PR-4 Use Limitation • PR-5 Data Quality • PR-6 Individual Participation • PR-7 Security Safeguards • PR-8 Accountability.	The Fair Information Practice Principles were added to the standard to reflect industry best practices.
47	Appendix C, Page C-20	Added an overview before the table describing the Procedures for Assessing Compliance with RT Security Standards.	Added to clarify that the second section of the Appendix focuses on assessing the minimum controls.
48	Appendix C, Pages C-171 and C-172	Added assessment procedures for the privacy controls (PR-1 through PR-8).	The Fair Information Practice Principles were added to the standard to reflect industry best practices.
49	Appendix D. Sample Attestation Report	Updated the language in the Independent Accountant's Report to indicate that the RT Standards were used as the basis for the opinion.	Updated to better reflect the process used by the auditor in performing the attestation review.
50	Appendix F References	Added a reference to the Fair Information Practice Principles.	The Fair Information Practice Principles were added to the standard to reflect industry best practices.

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security

RT
Registered Traveler™